HW 5 Solutions Fall 2023

Q1 When $F_{16} = F_2[x] \pmod{\underbrace{x^4+x^3+x^2+x+1}_{P(x)}}$ s.t. $P(\alpha)=0$.

Then one can brute force to find all primitive elements. You can also do some cheating. Since we already know that x^4+x^3+1 = primitive polynomial any β s.t. $\beta^4+\beta^3+1=0$ is a primitive element. Look at my trick in the singular file "find-primitive.sing", where I find 4 PEs.

$\beta = \alpha+1$, or α^2+1, α^3+1, $\alpha^3+\alpha^2+\alpha$

Q2 This is easy. Note that the only irreducible polynomial of degree 2 is $x^2+x+1 = P(x)$.

$P(\beta)=0$. If $\beta \in F_4 = \{0, 1, \alpha^5, \alpha^{10}\}$

where α = PE of F_{16}.

$$P(\beta)=0 \Rightarrow \beta^2+\beta+1. \text{ If } \beta=\alpha^5$$

$$\Rightarrow (\alpha^5)^2+\alpha^5+1 = \alpha^{10}+\alpha^5+1$$

$$= 0 \pmod{\alpha^4+\alpha^3+1}$$

When $\beta = \alpha^{10}$.

$$\beta^2+\beta+1 = \alpha^{20}+\alpha^{10}+1 = 0 \pmod{\alpha^4+\alpha^3+1}.$$

Q3 The expression is given in the HW: for $p=2$

$$(\alpha_1 + \cdots + \alpha_t)^{2^i} = \alpha_1^{2^i} + \cdots + \alpha_t^{2^i}$$

but it is actually true for any prime power.

$$(\alpha_1 + \cdots + \alpha_t)^{p^k} = \alpha_1^{p^k} + \cdots + \alpha_t^{p^k}$$ for any field of characteristic p, i.e. for $\mathbb{F}_{p^k}$

Proof: put $t=2$: $$(\alpha_1 + \alpha_2)^{p^k} = \alpha_1^{p^k} + \alpha_2^{p^k} \quad — (1)$$

Set $k=1$. As I gave in the hint

$$(\alpha_1 + \alpha_2)^p = \alpha_1^p + \binom{p}{1}\alpha_1^{p-1}\cdot\alpha_2 + \cdots + \binom{p}{p-1}\alpha_1\cdot\alpha_2^{p-1} + \alpha_2^p$$

Since the binomial coefficients $\binom{p}{i}$ are multiples of p, they are $\equiv 0 \pmod p$. So.

$$\underbrace{(\alpha_1+\alpha_2)^p = \alpha_1^p + \alpha_2^p}_{\text{for } k=1} \quad — (2)$$

Raise Eqn (1) to the p^{th} power:

$$\left[(\alpha_1+\alpha_2)^{p^k}\right]^p = (\alpha_1^{p^k})^p + (\alpha_2^{p^k})^p$$

$$\Rightarrow \quad (\alpha_1+\alpha_2)^{p^{k+1}} = \alpha_1^{p^{k+1}} + \alpha_2^{p^{k+1}} \quad — (3)$$

$\Rightarrow$ Eqn. (1) being true for k, Eqn (3) makes it true for $k=k+1$, Hence Eqn (1) is true by induction.

Now $(\alpha_1+\alpha_2+\alpha_3) = [\underbrace{(\alpha_1+\alpha_2)}_{\alpha} + \alpha_3]$ ... and so on ...

Q4 Design of a 3-bit Mastrovito Multiplier.

$F_8 = F_2[x] \pmod{P(x) = x^3 + x + 1}$

$$\alpha^3 + \alpha + 1 = 0 \Rightarrow \alpha^3 = \alpha + 1$$
$$\alpha^4 = \alpha^2 + \alpha$$

$Z = A \cdot B$. $\quad A = a_0 + a_1\alpha + a_2\alpha^2$

$B = b_0 + b_1\alpha + b_2\alpha^2$

$$A \cdot B = \left(\sum_{i=0}^{2} a_i\alpha^i\right) \cdot \left(\sum_{i=0}^{2} b_i\alpha^i\right) = (a_0 + a_1\alpha + a_2\alpha^2)(b_0 + b_1\alpha + b_2\alpha^2)$$

$$= a_0b_0 + a_0b_1\alpha + a_0b_2\alpha^2 + a_1b_0\alpha + a_1b_1\alpha^2 + a_1b_2\alpha^3 + a_2b_0\alpha^2 + a_2b_1\alpha^3 + a_2b_2\alpha^4$$

$$= \begin{pmatrix} a_0b_0 \\ + \\ a_1b_2 \\ + \\ a_2b_1 \end{pmatrix} + \begin{pmatrix} a_0b_1 \\ + \\ a_1b_0 \\ + \\ a_1b_2 \\ + \\ a_2b_1 \\ + \\ a_2b_2 \end{pmatrix}\alpha + \begin{pmatrix} a_0b_2 \\ + \\ a_1b_1 \\ + \\ a_2b_0 \\ + \\ a_2b_2 \end{pmatrix}\alpha^2$$

$$= z_0 + z_1\alpha + z_2\alpha^2$$

[See the singular file of the design + miter]

Q5 Just apply the lagrangian interpolation formula & make use of Singular to Compute the polynomial. In fact, the "interpolate.sing" file that I had uploaded on the website can be easily modified to update the function values @ $\frac{N_i}{D_i} f(x_i)$

$i = 1 \ldots 8$.

Interpolated polynomial is:

$$f(A) = (\alpha^2+\alpha+1) A^7 + (\alpha^2+1) \cdot A^6 + \alpha \cdot A^5 + (\alpha+1) A^4 + (\alpha^2+\alpha+1) A^3 + (\alpha^2+1) \cdot A$$

Note, for random logic abstraction in $\mathbb{F}_q$, the polynomial is of degree $q-1$, & is quite dense. Random logic is better dealt by ABC.

See singular file "hw3-q5-lagrange.sing" on the website.